How to protect e-wallet from KYC frauds

By Bindisha Sarang

InfrasoftTech
Fintech Digital Solutions

Media Coverage
21 February 2020 | Rediff.com

The KYC fraud has become so rampant that Delhi Police's Twitter account has issued a word of warning, points out Bindisha Sarang.

Financial frauds are not new. They are a hydra-headed problem cut one off, more spring in their place

.

For instance, a 73-year-old Paytm customer from Mumbai lost Rs 1.7 lakh recently via know-your-customer (KYC) fraud. The latest type of fraud to hit e-wallets is the KYC fraud.

Modus operandi

The Reserve Bank of India has made KYC mandatory for mobile wallet users. Scammers have used KYC as an entry point. Usually, the victim gets a text message stating his e-wallet needs to be KYC compliant; he is asked to call the telephone number provided in the message.

To update the KYC, he is asked to download an app, usually TeamViewer Quick Support or AnyDesk -- these are remote access control mobile apps. The phishers ask you to transfer Rs 1 to check the status of the e-wallet.

While the customer is entering a password or PIN for his e-wallet, the scammers are collecting details being entered alongside. They now have access to your mobile wallet ID and password. Soon your bank account is linked to the mobile. The wallet is debited to other accounts using different transactions.

What to do

The KYC fraud has become so rampant that Delhi police's Twitter account has issued a word of warning. Says Aagashe, "The KYC update will never happen via a third-party app.

If it has to happen on any app, it will happen within the original e-wallet app itself." Some e-wallets like Paytm have blocked its users from using the platform if they have apps like TeamViewer and AnyDesk on their smartphones.

Users get a pop-up message on Paytm, asking them to uninstall these remote access apps before they start using the wallet.

Tips to prevent other types of frauds

Unified payments interface (UPI) has a feature where you or the merchant can send the user a request to collect money.

Rajesh Mirjankar, managing director (MD) and chief executive officer, InfrasoftTech,
says, "Use digital payment modes only on trusted and verified websites. Remember that for UPI transactions, the PIN is never asked on the merchant site. It is always entered on your PSP app. Also, note that the credit transaction does not need the client to provide a mobile PIN."

Remember you don't need to authorise a transaction if the money is being transferred to your account, but the fraudster makes you believe you do and you end up sharing the PIN, and your hard-earned money gets re-routed.

Sanjay Katkar, joint MD and chief technology officer, Quick Heal Technologies, says, "The mobile app claiming to speed up your smartphone actually wants to wrest control of your phone and sniff out all the stored passwords."

Another method fraudsters use is by spreading fake customer care numbers for banks or UPI platforms online.

And when you run a search online, you often end up calling these numbers. Visit a bank or type out the whole URL to avoid being scammed.

Coverage : Rediff.com